REMARKS

Claims 1, 12 and 20 have been amended. Claims 4, 6, 10, 11, and 18 were previously canceled. Accordingly, claims 1 - 3, 5, 7 - 9, 12 - 17, and 19 - 29 are currently pending in the application and are presented for reconsideration and reexamination in view of the following remarks.

In the Office Action, claims 1, 12, and 20 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,747,564 to Mimura et al.; claims 1, 12, and 20 were rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 5,120,939 to Claus et al. in view of U.S. Patent Application Publication No. 2003/0025599 to Monroe; claims 1 - 3, 5, 7 - 9, 12 - 17, and 19 were rejected under 35 U.S.C. §103(a) as unpatentable over U.S. Patent No. 6,732,278 to Baird, III et al. in view of Monroe; and claims 20 - 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Baird, III et al. in view of U.S. Patent Application Publication No. 2002/0104006 to Boate et al. and Monroe.

By this Response and Amendment, the Examiner's rejections have been traversed. Support for the amendments to claims 1, 12, and 20 can be found for example, in the specification in the Summary of the Invention, at page 9, lines 10 - 15, page 10, lines 5 -7, page 12, lines 3 - 6, page 12, line 15 to page 13, line 2, page 13, lines 3 - 10, page 16, line 17 to page 17, line 3, page 17, lines 9 - 15.

It is therefore respectfully submitted that the above amendments introduce no new matter within the meaning of 35 U.S.C. § 132.

Rejection under 35 U.S.C. § 102(e)

The Examiner rejected claims 1, 12, and 20 as being anticipated by Mimura et al.

Response

Reconsideration and withdrawal of the rejection are respectfully requested.

For a reference to anticipate an invention, all of the elements of the claimed invention must be present in the reference. The test for anticipation under section 102 is whether each and every element as set forth in the claims is found, either expressly or inherently, in a single prior art reference. *Verdegaal Bros. V. Union Oil Co. of California,* 2 USPQ2d 1051, 1053 (Fed. Cir. 1987. The identical invention must be shown in as complete detail as is contained in the claim. *Richardson v. Suzuki Motor Co.,* 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must also be arranged as required by the claim. *In re Bond,* 15 USPQ2d 1566 (Fed. Cir. 1990).

Applicants submit that Mimura et al. fails to disclose each and every element of independent claims 1, 12, and 20, as amended.

The present invention overcomes a disadvantage of the prior art by continually validating and reviewing personnel access. *See* for example, page 12, line 15 to page 13, line 2.

Independent claim 1 recites, *inter alia*:

"...providing processor-based physical asset protection by triggering a user status change...;

...making access decisions in accordance with usage patterns of the user by using the integration of the processor based physical asset protection and processor based information asset protection to grant rights to the information systems...the information asset protection reflects the user status change updated to reflect changes in security access requirements; and transmitting a

breach of physical asset protection in the centrally-located hosted environment such that information asset protection is maintained by denying access thereto." (*emphasis added*).

Independent claim 12 recites, *inter alia*:

"...a physical asset protection module that provides physical protection for said asset by triggering a user status change...; ...the integrator providing integration of the physical protection and information from the information asset protection module for making access decisions in accordance with usage patterns of the user to grant rights to the information systems...the information asset protection reflects the user status change updated to reflect changes in security access requirements; and a transmitter for maintaining information asset protection by denying access to the information asset in the centrally-located hosted environment when there is a breach of the physical asset protection." (*emphasis added*).

Independent claim 20 recites, *inter alia*:

"...a processor based physical asset protection module transmitting a first signal to a centrally-located hosted environment, said first signal comprising user registration characteristics such that a user status change is triggered...;...and using an integration...for making access decisions in accordance with usage patterns of the user to grant rights to the information systems...the information asset protection reflects the user status change updated to reflect changes in security access requirements." (*emphasis added*).

Mimura et al. discloses a security guarantee method and system. Mimura et al. provides a security system for a door 130 of a building 105 of which staff that are authorized in advance can enter and leave and a door 140 for a computer room 110. The security system protects a database

and host computer 150 inside computer room 110. Entry/exit in/out of the computer room 110 and access to the computer system is guarded by a higher level of security than entry/exit in/out of the building 105. An internal door management device 155 controls opening/closing of the internal door 140 of the computer room 110. An access management device 185 executes an authentication processing of a correct person by fingerprint information of each terminal 165. *See* column 4, lines 20 - 57.

In step 545 in Figure 5, the internal door management device 155 permits or rejects the admission of the staff to the computer room 110 in accordance with the fingerprint verification result, and the host computer permits or rejects utilization of the application and the database in accordance with the fingerprint verification result. *See* column 7, lines 58 to column 8, line 26.

However, in Mimura et al. there is no processor-based physical asset protection by triggering a user status change upon valid entry/exit through a door of a building, and no information asset protection reflected by the user status change updated to reflect changes in security access requirements, as recited in independent claims 1, 12, and 20 of the present invention. Instead, the fingerprint verification result merely protects the entry/exit access to the computer room 110 through door 140 and the utilization of the application and the database. Staff is still required to log-on to terminal 165 to enter the computer room 110 and to use the application and the database. In contrast, in the present invention, a personnel access database is updated once an authorized user has left or entered the door of a building and permits/denies access to information technology in accordance with the updated status of the authorized user. *See* specification for example, at page 12, lines 3 - 6. Therefore, in Mimura et al. valid entry through door 130 does not

trigger a user status change to permit access to the assets, including door 140, and the application and database.

Mimura et al. also does not make access decisions in accordance with usage patterns of the user by using the integration of the processor to grant rights to the information systems as recited in independent claims 1, 12, and 20. Instead, access decisions are made in accordance with smart card 200 and log-on to terminal 165. The access management device 185 records the staff number 215 and the admission of the staff to the log file 180. Further, receiving the staff number, the access management device 185 deletes the staff information, including the staff number and the fingerprint information, and records leaving of the staff into the log file 189. *See* column 6, lines 39 - 50 and column 8, lines 49 - 54. Therefore, Mimura et al. does not maintain a history of the usage patterns to make access decisions regarding access to the application and database. Instead, Mimura et al. deletes the usage information.

Further, Mimura et al. does not transmit a breach of physical asset protection in the centrally-located hosted environment such that information asset protection is maintained by denying access thereto as recited in independent claims 1, 12, and 20. Instead, if mutual verification proves unsuccessful, processing entry through door 130 is finished. *See* column 5, line 58 to column 6, line 63. If the fingerprint verification result is the verification failure, processing log-on at terminal 165 is finished. *See* column 7, lines 2 - 31. If the fingerprint verification result is the verification failure, the internal door 140 is not opened and the utilization of the application and the database is not permitted. *See* column 7, line 58 to column

8, line 26. Therefore, the breach is not transmitted in Mimura et al.; it merely results in a denial of access.

Therefore, as Mimura et al. fails to teach or suggest each and every element of independent claims 1, 12, and 20, namely, triggering a user status change; making access decisions in accordance with usage patterns of the user to grant rights to the information systems; an information asset protection that reflects the user status change updated to reflect changes in security access requirements; and transmitting a breach of physical asset protection, Applicants submit that the reference fails to anticipate the independent claims, as amended.

Accordingly, Applicants respectfully request that the rejection of claims 1, 12, and 20 under 35 U.S.C. § 102(e) be withdrawn.

Rejections under 35 U.S.C. § 103(a)

Reconsideration and withdrawal of the rejection are respectfully requested.

To establish a *prima facie* case of obviousness, the Examiner must establish: (1) some suggestion or motivation to modify the references exists; (2) a reasonable expectation of success; and (3) the prior art references teach or suggest all of the claim limitations. *Amgen, Inc. v. Chugai Pharm. Co.*, 18 USPQ2d 1016, 1023 (Fed. Cir. 1991); *In re Fine,* 5 USPQ2d 1596, 1598 (Fed. Cir. 1988); *In re Wilson*, 165 USPQ 494, 496 (CCPA 1970).

Applicant respectfully submits that the combination of references fails to disclose, teach, or suggest all of the features of the claims.

1. The Examiner rejected claims 1, 12, and 20 as being unpatentable over Claus et al. in view of Monroe.

Response

Claus et al. discloses a databaseless security system. Door 830 provides entry to a secure location such as a room or a building. In order to obtain access, a user inserts a key 500 (smart card) into slot 810 and enters a password using switches 120. If the entered password matches the stored password, the key transmits its ID number to application station 990. If the key is authenticated, power is applied to the electric strike 995 via processor 760 which enables door to be pulled open. Processor 760 stores a list of lost/stolen keys and ID numbers that have been granted access to the facility over some time period. *See* column 11, lines 1 - 48. Application station 990 is a station, terminal, or machine that interacts with reader/writer unit 900 to selectively grant access to resources. *See* column 9, lines 48 - 65. The smart card may be used in connection with a plurality of authentication devices. *See* column 11, line 50 to column 12, line 4. Claus et al. eliminates the need to store and administer identification information regarding each user entitled to access to the protected resources. *See* column 3, liens 32 - 40.

However, in Claus et al. there is no processor-based physical asset protection by triggering a user status change upon valid entry/exit through a door of a building, and no information asset protection reflected by the user status change updated to reflect changes in security access requirements, as recited in independent claims 1, 12, and 20 of the present invention. Instead, the processor 760 stores a list of lost/stolen keys and ID numbers that have been granted access to the facility over some time period. In contrast, in the present invention, a personnel access database is

updated once an authorized user has left or entered the door of a building and permits/denies access to information technology in accordance with the updated status of the authorized user. *See* published specification at paragraphs [0052] - [0054]. Therefore, in Claus et al. valid entry through a door 830 does not trigger a user status change to permit access to resources.

Claus et al. also does not make access decisions in accordance with usage patterns of the user by using the integration of the processor to grant rights to the information systems as recited in independent claims 1, 12, and 20. Instead, access decisions are made in accordance with key 500 (smart card) into slot 810 and entering a password using switches 120. Therefore, Claus et al. does not maintain a history of the usage patterns to make access decisions regarding access to the room of a building.

Further, Claus et al. does not transmit a breach of physical asset protection in the centrally-located hosted environment such that information asset protection is maintained by denying access thereto as recited in independent claims 1, 12, and 20. Instead, there is no discussion anywhere in the reference of what happens when there is a breach of physical asset protection.

The Examiner cites Monroe in attempt to cure the deficiencies of Claus et al. regarding the information asset protection reflecting the user status change updated to reflect changes in security access requirements.

Monroe teaches a method and apparatus for collecting, sending, archiving and retrieving motion video and still images and notification of detected events. The method and apparatus are for identifying the occurrence of an event at a remote location. *See* Abstract. One of the objects

of the invention is to log an image of personnel attempting to gain access through an access control system, and to log all successful entry attempts and all unsuccessful attempts. *See* paragraph [0050].

Even *assuming arguendo* that Monroe teaches updating a user status change, Monroe fails to cure the deficiencies of Claus et al. because of the following.

The Monroe reference fails to teach or suggest information asset protection that reflects a user status change updated to reflect changes in security access requirements as recited in amended independent claims 1, 12, and 20 of the present invention. Instead, in Monroe, there is no information asset protection discussed anywhere in the reference. Monroe merely permits structured and controlled notification based on the identification of events as they occur. *See* paragraph [0024]. Monroe provides digital surveillance information collection at a remote location rather than in an integrated centrally-located hosted environment as recited in amended independent claims 1, 12, and 20. In contrast, the present invention makes access decisions in accordance with usage patterns of the user by using the integration of the processor based physical asset protection and processor based information asset protection to grant rights to the information systems.

2. The Examiner rejected claims 1 - 3, 5, 7 -9, 12 - 17, and 19 as being unpatentable over Baird, III et al. in view of Monroe.

Response

Reconsideration and withdrawal of the rejection are respectfully requested.

Baird, III et al. discloses an apparatus and method for authenticating access to a network resource. For maximum security, database 408 can be configured to require an account password to be changed at each log-in. *See* column 7, line 63 to column 8, line 21. If the untrusted computer is compromised by a virus or other malicious code, the computer can send anything to the smart card in lieu of sending the document viewed by the user. A user is authenticated to device 101 by three authentication factors: what the user has (the particular device 101), what the user knows (the global password), and what the user is (the biometrics). If the user does not have the correct device 101 then the device the user does have has an incorrect device-dependent key and the user will be denied access. *See* column 16, line 39 to column 17, lines - 26. A device preference sets a limit on the time available to authenticate to the device 101 and/or the number of permitted authenticate attempts. *See* column 17, lines 32 - 58. Even if the attacker coerces the user to provide the biometrics, the user can enter the duress password at step 606 and thereby safely deny the attacker access to the important accounts. *See* column 18, lines 27 - 45.

However, in Baird, III et al. there is no processor-based physical asset protection by triggering a user status change upon valid entry/exit through a door of a building, and no information asset protection reflected by the user status change updated to reflect changes in security access requirements, as recited in independent claims 1 and 12 of the present invention. Instead, there is no discussion anywhere in the reference of triggering a user status change or entering/exiting the door of a building.

Baird, III et al. also does not make access decisions in accordance with usage patterns of the user by using the integration of the processor to grant rights to the information systems as

recited in independent claims 1 and 12. Instead, access decisions are made in accordance with setting a device preference limit on the time available to authenticate to the device 101 and/or the number of permitted authenticate attempts. Therefore, Baird, III et al. does not maintain a history of the usage patterns to make access decisions regarding access to the device.

Further, Baird, III et al. does not transmit a breach of physical asset protection in a centrally-located hosted environment such that information asset protection is maintained by denying access thereto as recited in independent claims 1 and 12. Instead, there is no discussion anywhere in the reference of transmitting a breach of physical asset protection.

The Examiner cites Monroe in an attempt to cure the deficiencies of Baird, III et al. regarding triggering a user status change upon valid entry or exit through a door of a building.

Monroe teaches a method and apparatus for collecting, sending, archiving and retrieving motion video and still images and notification of detected events. Even *assuming arguendo* that Monroe teaches updating a user status change, Monroe fails to cure the deficiencies of Baird, III et al. because the reference fails to teach or suggest information asset protection that reflects a user status change updated to reflect changes in security access requirements as recited in amended independent claims 1 and 12 of the present invention. Instead, in Monroe, there is no discussion of information asset protection anywhere in the reference. Monroe merely permits structured and controlled notification based on the identification of events as they occur. *See* paragraph [0024]. Monroe merely provides digital surveillance information collection in a remote location. In contrast, the present invention makes access decisions in accordance with usage patterns of the user by using the integration of the processor based physical asset

and withdraw the outstanding rejections under 35 U.S.C. §103(a). Moreover, as dependent claims 2, 3, 5, 7 – 9, 13 – 17 and 21 – 29 depend from on of claims 1, 12 and 20, Applicants submit that these claims are also allowable for at least similar reasons.

CONCLUSION

In light of the foregoing, Applicants submit that the application is now in condition for allowance. If the Examiner believes that the application is not in condition for allowance, Applicant respectfully requests that the Examiner call the undersigned attorney.

Respectfully submitted,
NATH & ASSOCIATES, PLLC

July 3, 2006

NATH & ASSOCIATES, PLLC
112 South West Street
Alexandria, VA 22314-2891
Tel: 703-548-6284
Fax: 703-683-8396

Gary M. Nath
Registration No. 26,965
Gregory B. Kang
Registration No. 45,273
Teresa M. Arroyo
Registration No. 50,015
Customer No. 20529